CHAPTER II

LITERATURE REVIEW

Testing and assessment remain an integral part of instructional systems design for traditional classroom based courses as well as web-based training courses. The goal of testing is to determine if learning objectives have been accomplished.[1] The Internet offers an alternative medium for assessment. Web-based assessment that can be provided through the Internet provide greater accessibility, automation on question delivery and submission and faster result.

2.1 Web-based Assessment Solution Development

There are two approach in developing web-based assessments solution, client side scripting language and server side scripting language. To develop a client side web-based assessment, JavaScript is a standard scripting language commonly used today that continues to be very popular since it works with all browsers that use a graphical user interface. Server side processing on the other end relies on a back end machine to calculate test results and return the output in HTML format to the user. A non-proprietary technology called Common Gateway Interface (CGI) is used to implement server based assessment. [1]

2.2 Web-based Examination Available on the Internet

A number of web-based assessment solution web page were found in the Internet. One of the major assessment provider is Educational Testing Service (ETS) which provide web-based assessment solution for TOEFL and GRE while the others offer customized assessment solution with WYSIWYG assessment editor included for their potential client over the Internet.

2.2.1 Educational Testing Service

Educational Testing Service (ETS) primary purpose has been the development of tests and other assessment tools to provide information (including test scores and interpretative data) to test takers, educational institutions, and others who require this information.[2] As the pioneer of computer-based testing, ETS able to cater convenient scheduling and fast scores for test taker. ETS had also developed Test Creation Assistant, which automates item writing according to guidelines set by experienced test developers and content experts. One of the latest assessment feature of web-based testing provide by ETS is evidence-centered design platform, which allows customized tests to be administered in real time to student. The ETS also working on the possibilities of assessment application that will incorporate diagnostic feedback to help test takers improve their knowledge and skills and access to educational opportunities.

2.2.2 Questionmark

Questionmark is another computer aided assessment service provider. Under the Questionmark Perception trade mark, they provide assessment solution packaged for stand alone computer using Windows environment and web-based solution that can be reached through the Internet.. Perception for Windows is used to create, deliver and report on assessments using the Windows PC platform.. Perception for Web, on the other hand is used to administer assessments using the Internet or Intranets.[3]

Questionmark Perception come with a WYSIWYG editor that help to create and deliver tests, quizzes and surveys on Intranets as well as in the Internet or on a standalone personal computer running Windows operating system. With a built in wizard, Questionmark enable their client to easily create item banks, questions stored in the item bank can be randomized and shuffled to individualize assessments and the html templates can be selected to specify the look and feel of the assessment web page as required. MS Access and SQL (Microsoft or Oracle) database can be used to store answers, scores, and results. To overcome the security issues, especially for the high stakes examinations, where the content is valuable, Questionmark provide the Perception Secure Browser to limit printing, navigation and save-to-disk functions.[4]

2.2.3 Pastel Software

Pastel Software introduced a web-based software program that allows candidates to write standard examinations for certificates of competency in accounting and payroll

software packages. The examination candidates can go to any one of Pastel certified examination centers, pay the examination fee, log onto the web and write the exam.[5]

Based on a series of questions with multiple-choice answers, the examination is electronically "marked" as soon as the candidate completes the last question and submits the examination. Candidates who achieve passing scores then receive the relevant confirmation of competency within minutes. Certificates will be dispatched from Pastel Software and will reach the candidate within 48 hours.

Pastel examinations that can be written on the web include Pastel Partner Accounting, Advanced Pastel Partner Accounting, Pastel Payroll, Pastel Accounting SOHO V2, and a number of reseller qualifications such as the Pastel Certified Installer (PCI). As with all Pastel accounting software, the examinations will be offered in a various languages so that candidates can write in the language of their preference. Currently, a choice of English or Afrikaans is offered in South Africa. The system opens up opportunities for schools, and colleges to offer the web-based examination facilities and generate revenue.

2.2.4 The Computer-based TOEFL Test

The purpose of the TOEFL® test is to evaluate the English proficiency of people whose native language is not English. It also provides English proficiency testing services for international students planning to study in the United States, Canada, or other countries where English is the language of instruction. TOEFL is used by

institutions in countries where English is the language of instruction. In addition, government agencies, scholarship programs, and licensing/certification agencies use TOEFL scores to evaluate English proficiency. [6]

The TOEFL test was introduced as a computer-based test in July 1998. TOEFL web-based assessment solution is provided by ETS. It combines many of the same question types as the traditional paper-based test with new question types that can be offered only on the computer. The test is offered on computer throughout most regions of the world.

Computer added testing enabled TOEFL to implement value added services to their conventional testing. Among the improvements included are:

Stimuli in the **Listening** section are accompanied by visuals that set the scene, provide clues to the speakers' roles, or illustrate topics. This innovation broadens the components available to create varied and interactive stimuli that more closely approximate actual listening experiences, such as classroom lectures or campus conversations.

New item types in Listening require examinees to demonstrate their English proficiency by interacting with the information presented to them. Examinees must use integrated language skills to manipulate graphics, categorize information, and order the elements in a process.

New item types in Reading offer more than four options and require examinees to demonstrate their comprehension of a passage by manipulating the language in several ways. Examinees identify words or phrases with similar meanings, demonstrating their ability to comprehend discrete language segments and to use context clues. They highlight information in the passages to demonstrate their comprehension of main ideas and supporting details. They also identify paraphrases and inferences to demonstrate the ability to analyze meaning. Finally, they insert an extra sentence into the appropriate part of a passage, a task that demonstrates a more cognitively complex aspect of comprehension: the ability to understand the rhetorical organization of a passage, including elements of coherence and cohesion.

A Writing section requires examinees to compose an essay in English in response to an assigned topic. This measure enables examinees to demonstrate their ability to generate, organize, and develop ideas and to support those ideas with examples or evidence. This section directly measures the examinees' ability to produce written language, and complements the information obtained from the Structure section.[6]

On security issues, Toefl has deployed additional security measurement such as allowing fewer examinees test at one time and those who do are monitored by two proctors as well as by video equipment.

2.3 Understanding the World Wide Web (WWW)

To implement a web-based solution, it is important to understand the Internet service that the assessment solution will be deployed on. WWW is a distributed hypermedia

technology that was initially proposed by Tim Berners-Lee at the European Laboratory for Particle Physics (CERN) in 1989 to facilitate the international exchange of research findings using the Internet.[7] Two years later, a prototype World Wide Web was developed at CERN using the NeXT computer as the platform. The first graphically oriented browser; Mosaic was developed at NCSA Center, University of Illinois by Mark Andrawson and others in 1993. Since then more than two million copies of Mosaic were delivered over the Internet.

Stalling and Van Slyke (1998) define the web as a system consisting of an internationally distributed collection of multimedia files supported by clients (user) and servers (information providers). Each file is addressed in consistent manners using its universal resource locator (URL). Clients can view files from providers using browsers such as Mosaic, Netscape and Internet Explorer. Hypertext Markup Language standard controls the layout of the browser display. Hypertext Markup Language defines embedded commands in text file which specify features of the browser display such as fonts, colors, images and their placement on the display and the site of the locations where the user can invoke the hyperlinks and their target. [7]
An individual WWW page may contain:

a) Text, graphic image and link to voice and video
b) Form for the user to fill out
c) Trigger a search for a database or a file
d) Information that is dynamically updated
e) Applets that can be transferred to a user's machine for execution

To enable host and server communication in the Internet, WWW uses Hyper Text Transfer Protocol (HTTP) as communication protocol above the TCP/IP networks for fetching files from appropriate servers as specified by the hyperlinks.

2.4 Web Security

One of the problem in implementation of a web solution is to maintain it security. As a public network, people with different intention access to the Internet network. To understand web security issues, Stein (1998) initially divided web connection into three components:

1. The web browser
2. The web server
3. The connection between the web browser and the web server [8]

From this division, he concluded that web security could also be divided into three different components accordingly. They are:

1. Client side security
2. Server side security
3. Document confidentiality

2.4.1 Client Side Security

Client side security as a measure that protects the user's privacy and the integrity of her computer. In client side security, technological solutions should include

safeguards to protect users against computer viruses and other malicious software, as well as measures that limit the amount of personal information that browsers can transmit without the user's consent. Stein also includes organization attempts to prevent employees' web browsing activities from compromising the secrecy of the company's confidential information or the integrity of its Local Area Network. Secure Socket Layer and Secure Electronic Transaction are two examples of client side security. [8]

2.4.1.1 Secure Sockets Layer (SSL)

Secure Sockets Layer is the dominant protocol for encrypting general communication between browser and server. It was first introduced in 1994 with the first version of Netscape Navigator browser. Microsoft starts supporting this protocol after the release of SSL v3.0 implemented in Internet Explorer 3.0. SSL is a session level protocol that can be used to encrypt transmissions on the World Wide Web. Any program that uses TCP can be modified to use secure SSL connections by making a few source code changes. SSL provides assurance of privacy by encrypting data, messages and server authentication and it can also demand client authentication. In implementing client side security, SSL uses two different protocols:

1. The SSL Record Protocol, which encapsulates everything that comes through, including the SSL Handshake Protocol Packet.

2. The SSL Handshake Protocol, which is used to negotiate and establish security methods and parameters. [9]

2.4.1.2 Secure Electronic Transaction (SET)

SET is a cryptographic protocol jointly developed by Visa, Mastercard, Netscape and Microsoft. It is specifically developed to secure credit and debit card transactions between customers and merchants. Among essential services provided by SET protocol are:

1. Authentication. All the parties in the credit card transaction are authenticated using digital signatures. This includes the customer, the merchant, the bank that issues the credit card and the bank that handles the merchant checking account.

2. Confidentiality. The transaction is encrypted to prevent packet-sniffing activity by eavesdroppers.

3. Linkage. SET allows a message sent to one party to contain an attachment to be read by another party to verify that the attachment is correct.

4. Message integrity. Devious individuals who wish to alter the account number or the amount of the transaction cannot tamper with the transaction.

2.4.2 Server-side Security

Server side securities are measures that protect the web server and the machine it runs on from break-ins, site vandalism and denial of service attacks, attacks that make the website unavailable for normal use. As most web servers can be connected through the Internet public network, it is thus exposed to threats. Stein identifies seven factors why web servers are vulnerable. There are:

1. Bugs in system software. Typical server software bugs appear when the server is exposed to a condition that its developer did not anticipate. Other bugs appear when software subsystems interact in unexpected way, such server that behaves strangely when the domain name system becomes inaccessible. Computer hackers on the other hand are on the constant lookout for bugs in computer software because each bug represents a potential portal of entry.

2. System software is incorrectly configured. The server hardware is not secure. One of vendors' marketing strategies to sell their product is to make the product user friendly and easy to install. As a result, a lot of popular network services are turned on by default, remote configuration facilities are enabled, and the policy accessing system files are made very liberal. Malicious users can exploit these by modifying the system and possibly expanding her access to the system.

3. Networks are not secure. Most transmission across the Internet and local area network are unencrypted. Anyone with the right access to the network and the right software can intercept messages with packet sniffers. One of the popular targets of packet sniffing is the user name and password with specially designed password sniffing program.

4. Open holes in Remote Authoring and Administration Tools. Updating web content in the server from remote site using remote authoring and administration tools make web administrator job more convenient and flexible but at the same time holes in the system may create an opportunity to intruders to gain access as administrator.

5. Insider threats are overlooked. Most security policies are concern with outsiders trying to break-in to the server and overlook the potential threats within the organization. It is possible for members of the organization to make unauthorized access to the server for unexpected purposes.

6. Denial-of- Service threats are often overlooked.

7. Lack of security policy. [8]

2.4.2.1 Firewall

A firewall is a system or group of systems utilized to enforce access control policy between two network entities. It determines which inside intranet services can be accessed by client from outside of the organization and which outside Internet sites can be viewed by the members of the organization intranet.

Fundamentally the firewall works on a pair of mechanisms:

a) To block traffic

b) To permit traffic

By blocking traffic, firewall prevents people on the outside from getting into the user's system. The most important aspect of a firewall is to allow the System Administrator to easily implement an access control policy. Four basic purposes of firewall deployments are:

1) To block incoming data that might contain a hacker attack.

2) To hide information of the network by implementing Network Address Translation (NAT). All out-going traffic is address with the firewall address rather than the network address.

3) To screen out-going traffic to limit Internet use and access to remote site.

4) To screen incoming traffic to prevent illegal intrusion and hacking activities.

2.4.3 Information Security

The proposed web-based assessment solution deployment involve the process of information retrieval and submission between the examination center and the Examination Syndicate web server. As the information traverse over the Internet medium, four fundamental objectives of information security must be highlighted. There are:

1) Confidentiality: Ensuring that information is not disclosed or revealed to unauthorized persons.
2) Integrity: Ensuring consistency of data; in particular, preventing unauthorized creation, alteration or destruction of data.
3) Availability: Ensuring that legitimate users are not unduly denies access to information resources
4) Legitimate use: Ensuring that resources are not used by unauthorized persons or in unauthorized way. [9]

2.5 Potential Threats to the Proposed Web-based Solution

In implementation of a web-based assessment solution, the potential threats that may compromised the assessment integrity must be identifies. The table below shows a typical network threats to information security. [10]

Threats	Description
Authorization violation *	A person authorized to use a system for one purpose use it for another unauthorized purposed.

Bypassing control *	An attacker exploits system flaws or security weakness
Denial of service *	Legitimate access to information or other resources is deliberately impeded.
Eavesdropping *	Information is revealed from monitored communication
EM/RF interception	Information is extracted from radio frequency or other electromagnetic field emanation from electronic or electromechanical equipment
Illegitimate use	A resource is use by unauthorized person or entity.
Indiscretions by personnel	An authorized person discloses information to an unauthorized person, e.g. for money or favors, or through carelessness
Information leakage *	Information is disclosed or revealed to an unauthorized person or entity.
Integrity violation *	The consistency of data is compromised through unauthorized creation, modification or destruction of data
Intercept/alter *	A communicate data item is changed, deleted or substituted while in transit.
Masquerade *	An entity (person or system) pretend to be entity
Media scavenging	Information is obtain from discarded magnetic or printed media

Physical intrusion	An intruder gains access by circumventing physical control.
Replay *	A captured copy of a legitimately communicated data item is retransmitted for illegitimate process
Repudiation *	A party to a communication exchange later falsely denies that the exchange took place.
Resource exhaustion	A resource (e.g. access port) is deliberately used so heavily that service to other user is disrupted.
Service spoofing	A bogus system or system component aims to dupe legitimate users or system into voluntarily giving up sensitive information.
Theft	A security critical item, e.g. a token or identity card is stolen.
Traffic analysis *	Information is leaked to unauthorized entities through observation of communication traffic pattern.
Trapdoor	A feature is built into a system or system component such that the provision of specific input data allows security policy to be violated.
Trojan horse	Software that contain an invisible or apparently innocuous part which, when executed, compromised the security of it user.

* Threats that computer communication security can counter.

Table 2.1: Typical Network Threats (Source: Ford, 1994)

As describe in the table above, in a World Wide Web environment, data traverse from client machine to server machine and vice versa in a public network is exposed to numbers of threats. The threats if not properly manage may compromise information confidentiality. Several measures must be taken to protect private information from being disclosed to third parties. For effective security, counter measures from the different categories need to be used together. Risk management assists in making proper decision on implementing safeguard to information.

2.6 Understanding Virtual Private Network (VPN)

VPN is the approach chosen in implementing this web-based assessment solution for the Malaysian Secondary school. It is the Internet connection technology of making a private network path within the Internet. A virtual private network (VPN) allows two or more private networks to be connected over a publicly accessed network. VPN are similar to a wide area networks (WAN) or a securely encrypted tunnel, but the key feature of VPN is that they are able to use public networks like the Internet rather than rely on expensive, private leased lines. At the same time, VPN have the same security and encryption features as a private network, while taking the advantage of the economies of scale and remote accessibility of large public networks. [11]

The Virtual Private Network is aimed at achieving a secure communication across TCP/IP network. A private virtual path (virtually) is established to route the data through a TCP/IP network. Data is transmitted in a controlled tunnel. Packet is

encapsulated to ensure integrity. To avoid unauthorized user, VPN applies a strong authentication algorithm.

VPN connection is use as an inexpensive and secure way to connect the organization Local Area Network from a remote site. Before VPN the technology is available, the organization that wishes to establish a private network must hire dedicated leased lines from communication service provider. With the VPN, the organization can use Internet connection instead, which is relatively very much cheaper. The VPN technology also enables remote access to the organization server through Internet dial-in.

VPN into three categories. [11] There are:

1) Access VPN. Provides remote access to a corporate intranet or extranet over a shared infrastructure with the same policies as a private network. Access VPN enable users to access corporate resources whenever, wherever, and however they require. Access VPN encompass analog, dial, ISDN, Digital Subscriber Line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, or branch offices.

2) Intranet VPN. Links corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network,

including security, quality of service (QoS), manageability, and reliability.

3) Extranet VPN. Links customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, QoS, manageability, and reliability.

2.6.1 Virtual Private Network Protocol

There are at least four protocols being pitched for VPN which are:

1. Point-to-Point Tunneling Protocol (PPTP), a product of Microsoft.
2. Layer 2 Forwarding Protocol (L2F), developed by Cisco.
3. Layer 2 Tunneling Protocol (L2TP), and
4. IP Security (IPSec)

2.6.1.1 Tunneling

Tunneling is a protocol encapsulation, a practice of encasing one protocol in another protocol. A packet in one protocol is wrapped by another protocol for certain reasons like avoiding protocol restriction or applying encryption. For example, a connection oriented packet, i.e. Synchronized Data Link Control (SDLC) packet can be transmitted on TCP/IP connectionless path by wrapping the SDLC packet with

TCP/IP header. A tunnel provides a way to encapsulate packets of a passenger protocol inside a transport protocol. There are several situations where tunneling is useful, such as allowing multiprotocol local networks to communicate over a single-protocol backbone, connecting partitioned sub-networks, and allowing virtual private networks across wide-area networks. Tunneling involves three types of protocols:

1. The *passenger protocol* is the protocol being encapsulated; in a dial up scenario, this protocol could be Point-To-Point (PPP), Serial Line Internet Protocol (SLIP), or text dialog.

2. The *encapsulating protocol* is used to create, maintain, and tear down the tunnel. Cisco supports several encapsulating protocols, including the L2F protocol, which is used for virtual dial up services.

3. The *carrier protocol* is used to carry the encapsulated protocol; IP is the first carrier protocol used by the L2F protocol because of its robust routing capabilities, ubiquitous support across different media, and deployment within the Internet . [12]

PPTP requires the establishment of a tunnel for each communicating client and server. [13] This tunnel is used to carry all user session PPP packets for sessions involving a given client and server in a remote access communication. A key, which is present in the Generic Routing Encryption (GRE) header, indicates which session a particular PPP packet belongs to. In this manner, PPP packets are multiplexed and demultiplexed over a single tunnel between a given remote access client and server

machine pair. The value to use in the key field is established by the call establishment procedure, which takes place on the control connection. [13]

The VPN applies tunneling for security purposes. Private data packets are secured using data encryption, authentication or integrity functions and are then encased in an IP packet. Two types of VPN tunneling being proposed are:

1. Layer 2 tunneling (Data Link Layer), applied by PPTP, L2F and L2TP.
2. Layer 3 tunneling (Network Layer), applied by IPSec.

2.6.1.2 Point-to-point Tunneling Protocol

Point-To-Point Tunneling Protocol (PPTP) is a network protocol that enables a secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP based data network. The networking technology of PPTP is an extension of the remote access Point-To-Point Protocol (PPP). It encapsulates PPP packet into IP datagrams for information over the Internet or other public TCP/IP-based network. It can also be applied in private LAN-to-LAN networking.

A PPTP deployment involves at least three computers:

1. The PPTP client
2. The Network Access Server
3. The PPTP Server.

A client from a remote location establishes a connection to the Internet by connecting a network Access Server through a local Internet Service Provider like Jaring or TMNet. This connection can be done through Public Service Telephone Network (PSTNs) with a local rate telephone charge. Point-To-Point Protocol (PPP) is used for this connection. After the PPP connection is established, another dial up connection through this PPP to PPTP server is made to create a control connection that acts as a tunnel to channel the IP packet flow from a client to the enterprise server. The PPTP uses Generic Routing Encapsulation (GRE) Header to encapsulate the PPP packet within the datagram. Data are transmitted between client and PPTP server through this tunnel in form of IP datagram, which contains encapsulated PPP packet.

Hamzeh *et al.* (1999) define PPTP as a relationship between a PPTP Network Server (PNS) and PPTP Access Concentrator (PAC) on the client machine on a remote access environment. He describe the function of PPTP that specifies a call-control and management protocol, which allows the server to control access for dial-in circuit switched calls originating from a PSTN or ISDN. He divided PPTP into two parallel components:

1. Control Connection between each PAC-PNS pair operating over TCP
2. An IP tunnel operating between the same PAC-PNS pair, which is used to transport Generic Routing Protocol (GRE), encapsulated PPP packets for user sessions between the pair. [13]

Before PPP tunneling can occur between a PAC and PNS, a control connection must be established between them. The control connection is a standard TCP session over which PPTP call control and management information is passed. The control session is logically associated with, but separate from, the sessions being tunneled through a PPTP tunnel. For each PAC-PNS pair both a tunnel and a control connection exist. The control connection is responsible for establishment, management, and release of sessions carried through the tunnel. It is the means by which a PNS is notified of an incoming call at an associated PAC, as well as the means by which a PAC is instructed to place an outgoing dial call. [13]

Either the PNS or the PAC could establish a control connection. Following the establishment of the required TCP connection, the PNS and PAC establish the control connection using the Start-Control-Connection-Request and -Reply messages. These messages are also used to exchange information about basic operating capabilities of the PAC and PNS. Once the control connection is established, the PAC or PNS may initiate sessions by requesting outbound calls or responding to inbound requests. The control connection may communicate changes in operating characteristics of an individual user session with a Set-Link-Info message. Either the PAC or PNS may release individual sessions, also through Control Connection messages.

2.7 Potential Attack Against VPN Deployment

In a VPN deployment four type of network attack has been identifies. [14] There are:

a) Impersonation

b) Integrity

c) Disclosure

d) Denial of service

Impersonation attacks are those in which an attacker masquerades as another person. The strong authentication methods supported in PPTP can reduce the effectiveness of impersonation attacks. Successful *integrity* attacks result in the undetected modification of user data; for example, changing the contents of an electronic mail message in transit. Integrity attacks are generally impossible to prevent; the best that can be done is to detect the modification. Digital signatures of various types are useful defenses against integrity attacks. *Disclosure* attacks result in the exposure of data to an unintended person. The damage caused by disclosure attacks often depends on the content of the data revealed: A routine meeting request may have little value to an opponent, but the disclosure of confidential sales projections could be ruinous. The typical defense against disclosure attacks is the use of strong encryption to hide network traffic, which is available in PPTP. *Denial of service* attacks are the hardest attacks to defend against, and the easiest to perpetrate. The purpose of these attacks, as the name suggests, is to deny service to valid users.

Windows NT 4.0 has been hardened against a number of known denial of service attacks, including teardrop, newtear and syn flooding.[14]

2.8 The Examination Syndicate of Malaysia

The Examination Syndicate of Malaysia is a government agency under The Ministry of Education (MOE). It is the authorized body in managing public examinations for primary and secondary schools in Malaysia. The main objective of The Examination Syndicate of Malaysia is to plan, develop and administer education assessment parallel to National Education Policy. Under Section 67 Education Act 1996 (Act 550), the Minister delegates authority to the Director of The Examination Syndicate to run assessment for primary and secondary schools according to methods and standards defined by the Minister. Under Section 68 the same act, the Minister empowers Examination Syndicate Director to define:

a) Examination regulation
b) Time and location of the exam
c) Examination fees
d) Subject syllabus and medium of language for the examination.

2.9 Information Technology Subject for SPM Examination

The Information Technology subject was introduced to secondary schools in Malaysia in 1999. In the year 2000, 28 selected schools took part in the Information Technology Examination for Malaysian Certificate of Education (SPM). This is a

common test taken at national level at the same time and date but of different school location. For the first time in the Malaysian education system, an examination was administrated in a computer lab and students used computer applications to write out their responses to questions. Candidates' answer scripts were saved in diskettes and forwarded to the Examination Syndicate office through the State Education Department. A copy of the candidates' answer scripts was also sent to the Examination Syndicate office through File Transfer Protocol application over the Internet.

Certified teachers were selected among those teaching the Information Technology subject throughout the country to mark and score candidates' answer script. The teachers were centered at a computer lab and were given the candidates' diskette for marking. A scoring leader and a group of The Examination Syndicate officers helped them. The officer then processes the scores and issued the Information Technology subject results together with the result of other subjects on a single transcript.